(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
5 février 2004 (05.02.2004)

PCT

(10) Numéro de publication internationale
WO 2004/012372 A2

(51) Classification internationale des brevets[7] : H04L

(21) Numéro de la demande internationale :
PCT/FR2003/002364

(22) Date de dépôt international : 25 juillet 2003 (25.07.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/09475 26 juillet 2002 (26.07.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13420 Gémenos (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **CORON, Jean-Sébastien** [FR/FR]; 4 rue Léon Delagrange, F-75015 Paris (FR). **JOYE, Marc** [BE/FR]; 19 rue Voltaire, F-83640 Saint Zacharie (FR). **NACCACHE, David** [FR/FR]; 7 rue Chaptal, F-75009 Paris (FR). **PAILLIER, Pascal** [FR/FR]; 37 Cours de Vincennes, F-75020 Paris (FR).

(74) Mandataire : **NONNENMACHER, Bernard**; C/O Gemplus, Service Brevets, La Vigie, BP 90, F-13705 LA Ciotat Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** DATA ENCRYPTION METHOD, CRYPTOGRAPHIC SYSTEM AND ASSOCIATED COMPONENT

(54) **Titre :** PROCEDE DE CHIFFREMENT DE DONNEES, SYSTEME CRYPTOGRAPHIQUE ET COMPOSANT ASSOCIES

(57) **Abstract:** The invention concerns an encryption method, comprising a step which consists in formatting a clear message (m) with a formatting function (μ), and a step which consists in an exponentiation of the result of the preceding step using a public key (N, e) in accordance with the relationship $c = \mu(m)^e \bmod N$, c being an encrypted message, μ(m) being the result of the formatting step, and e and N elements of the public key. The invention is characterized in that the formatting function (μ) is The PSS function. The invention is applicable to cryptography, for example of RSA type, for smart cards for instance.

(57) **Abrégé :** L'invention concerne un procédé de chiffrement, comprenant une étape de formatage d'un message clair (m) par une fonction de formatage (μ), et une étape d'exponentiation du résultat de l'étape précédente à l'aide d'une clé publique (N, e) selon la relation $c = \mu(m)^e \bmod N$, c étant un message chiffré, μ(m) étant le résultat de l'étape de formatage, et e et N des éléments de la clé publique.Selon l'invention, la fonction de formatage (μ) est la fonction PSS. Application au domaine de la cryptographie, par exemple de type RSA, par exemple pour des cartes à puces.

WO 2004/012372 A2